

Business Snoops

and the

*Top 10 Spy Busting Tips
They Don't Want You To Know*



MANAGEMENT CONSULTANTS TO
BUSINESS & GOVERNMENT ON
ELECTRONIC EAVESDROPPING DETECTION
& BUSINESS ESPIONAGE PREVENTION

P.O. BOX 668, OLDWICK, NJ 08858 (USA)
908 • 832 • 7900 • 800 • 635 • 0811

Capabilities information — www.spybusters.com

(Services available throughout the U.S. and selected foreign countries.)

©1995-2002 Kevin D. Murray - CPP, CFE, BCPE

W *ho are these snoops?*
Competitors, vendors,

investigators, business intelligence consultants, activists, colleagues vying for positions, overbearing bosses, suspicious partners, the press, labor negotiators, government agencies... The list is long.

Why would I be a target?

Money and Power are the top two reasons behind illegal surveillance. If anything you say or write could increase someone else's wealth or influence, you are a target.

Is snooping common?

Yes. The news is full of stories about stolen information. In fact, many news stories themselves begin with leaks.

Can I protect myself?

Yes. Espionage is preventable. If you know the vulnerabilities, you can take the proper security precautions.


Some spy tricks are obvious...

Some are clever abuses of the new technology we live with every day. All are devastating.

Time has shown that many of the same tricks are used successfully over and over again. We present the top ten.

Prepare to fight back...




Kevin D. Murray — CPP, CFE, CCO, BCFE
Certified Protection Professional #3239
Certified Fraud Examiner #23707
Board Certified Forensic Examiner #3159

#1 – Trash Trawling...

Dumpster diving, waste archeology, or trashing, all refer to rifling garbage in an effort to cull valuable information. This is believed to be the number one method of business and personal espionage.

Surprise... In and of itself, stealing garbage is legal. The U. S. Supreme Court has confirmed that there is no expectation of privacy, or ownership, once an item is left for garbage pickup.

Scraps of seemingly useless information are synergistically related. The counterespionage process is one of reducing the availability of these puzzle parts. Shredding all waste paper is a major step in the protection process.

RECOMMENDATIONS & TIPS...

- Encourage the destruction of all waste paper.
- Purchase shredders appropriate for your needs.
- Use crosscut destruction for high levels of security.
- Computer paperwork and large volume waste require a central bulk shredder.
- Snoops love it when you save confidential papers in a cardboard box under the desk. Shred it now.
- Do not entrust wastepaper destruction to paper recycling vendors. Destroy it before recycling.
- Don't forget: you also need shredders next to copiers and in the executives' home offices.

THE BIG SHREDDER PURCHASING MISTAKE...

Buying just one large shredder for everyone to use.

Reason: Not everyone will use it.

Why?

Some people are too busy to be bothered. The better choice is several convenient desk-side shredders. This is one perk which has a very positive payback.

Bonus... Some companies promote their use of shredders to protecting their clients' privacy. — A service not offered by their competitors.

#2 – Bugs & Wiretaps

Although most snooping involves other methods listed in this booklet, electronic surveillance is the most devastating spy trick there is. Very private – and irrefutable – secrets are the target of this attack.

COMMON MISTAKE...

Saying, *“Oh, I’m just being paranoid,”* when you suspect electronic surveillance. Think... You wouldn’t be suspicious if everything were fine. Something is wrong.

COURSE OF ACTION...

- Do not discuss your suspicions with others unless they have a real need to know.
- Do not discuss suspicions in suspected areas.
- Do not attempt a do-it-yourself solution.
- Do not waste money buying spybuster toys.
- Seek professional guidance without delay.

Contrary to what you see on television, in the movies, or in catalogs, detection of bugs and wiretaps is equipment and knowledge intensive work.

Expect a professional sweep team to have about \$250,000+ dollars invested in their instrumentation. Their personnel will have deep experience in security, investigations, electronics and telecommunications.

HINT:

Don’t bother to check the yellow pages. Contact a corporate security director or professional security organization for a knowledgeable recommendation. It’s worth the effort.



**Bug parts...
on a quarter.**

#3 – The Drop By Spies

Check – and photocopy – the credentials and work orders of anyone performing technical work in or around your offices. Double check. Verify the work was actually requested and necessary.

This includes:

- telecommunications technicians,
- computer technicians,
- cleaning crews,
- office equipment repair persons,
- paper recyclers,
- electricians, et cetera.

Have someone representing your interests accompany these visitors while on your property. If possible, have them complete their work during normal business hours. Outside contractors and unauthorized company employees should never be allowed to roam unescorted within areas containing sensitive information.

One professional snoop brags openly that any building can be entered at any time, simply by posing as the air conditioning / heating guy.

His props include a clipboard with forms and an industrial thermometer. Optional: a 2-way radio and a hard hat. If challenged, he threatens not to come back for three weeks. Busy schedule, you know.

No one wants responsibility for denying this guy entry.

OTHER TIPS...

- Check your locks and alarm system regularly. Make sure each component really works. It is surprising how many effective-looking broken locks and alarms are relied upon for protection.
- If key control has long since gone out of control, tackle the problem now. Change locks and set up a system which will work. Consider card key access.
- When seeking assistance with security matters, be sure to hire consultants who don't also sell products, and who will not accept remuneration from companies they recommend.

#4 – Hacking & Cracking

Espionage aimed specifically at personal computers, laptop computers, networks and remote access ports is rampant. Explain to everyone who keeps sensitive data in their computers why security precautions are necessary.

Example: 'THE PROTECT YOUR LAPTOP AT ALL TIMES' RULE.

Replacement cost is not your only loss, consider the...

- valuable competitive and confidential data,
- time it took for someone to compile the data,
- time it will take to reconstruct the data,
- company's modem telephone numbers, and mainframe passwords stored on the drive. When this information is lost, the company is vulnerable to...
 - wholesale theft / corruption of mainframe data,
 - and sabotage via viruses, Trojan horses, etc.

Bottom line:

- Lower profitability.
- Reduced job security for everyone.

MORE COMPUTER SECURITY TIPS...

- Develop a communal sense of security responsibility.
- Limit physical access to computers by outsiders.
- Limit software access. Use quality passwords.
- Secure PC related materials; disks, backups, etc.
- Never leave an active terminal. Always log-off.
- Report suspected intrusions and altered data.
- Remove sensitive data from the PC when not in use.
- Protect memory media: floppies and optical disks.
- Copy commands can move sensitive data inadvertently.
- Do not rely on deletion commands. Use a wipe program instead.
- Erase diskettes before disposal, or transfer to other use.
- Disconnect PCs from networks when not in use.
- Computers using phone lines need access protection.
- Do not use unsolicited or borrowed software.
- Backup all data on a regular basis.
- Reformat hard drives before retiring old computers.
- Do not discuss system security with anyone you don't know – no matter what they tell you.

Q. What is the first rule of espionage?

*A. There are no rules.
If you have what they want,
they will use any means to get it.*

– M. Russell

#5 – Mobile Phone Leeches

Cellular and cordless telephones are among the easiest of eavesdropping targets. Contrary to common perception, reception of these conversations is generally crystal clear, without static or interference.

Each and every word can be understood. Use them with discretion.

Cellular radio-telephone communications can be received by the general public over hundreds of square miles. In addition to being an espionage windfall, monitoring of these transmissions has also become a national pastime with opportunistic hobbyists selling their 'finds' as well.

Monitoring of cellular and cordless telephone transmissions is illegal. Do not rely on the laws to protect your privacy, though. They are generally considered unenforceable.

New techniques in cellular eavesdropping include computer assisted, totally automated monitoring. This allows monitoring of specific phones, 24-hours a day, from cell to cell, without human assistance.

To protect car telephone conversations, arrange to call in on a number which is not answered with a company name or other identifying information. Use first names and code words to identify special projects. Speak in general and uninteresting terms.

Cordless telephones can be received up to one mile away. Use them only as an answering convenience. Switch to a regular telephone for increased – not absolute – security.

If you must have a cordless phone, buy one which operates in the **2.4 MHz** frequency range using **digital spread spectrum** technology.

Other telephones which can be monitored include:

- Commercial airline and rail telephones.
- Ocean liner phone calls.
- Long distance calls sent via satellite.
- Long distance calls sent via microwave radio links.

#6 – Technology Traitors

Technological advancements give us many communications conveniences. Portable telephones, for example. Unfortunately, they also bring new opportunities for the snoops.

Here are a few vulnerabilities you need to know...

- **Answering Machines.** Messages left on many home units can be remotely accessed using a simple two or three digit code. Easy to hack. Most people never change the code which comes preset in new machines. Some units also have a remote listen-in feature. Read your manual carefully.
- **Voice Mail.** The business version of an answering machine can also be monitored. Use the longest password possible. Change it often.
- **Baby Monitors.** In reality, very sensitive room bugs which transmit 24-hours a day. Monitored by passing burglars to see if the house is empty, and by nosy neighbors. Use monitors sparingly. Plug the transmitter into a light timer. Keep baby's door closed.
- **Fax Machines I.** Some fax machines use disposable rolls of black film in their printing process. Used rolls contain an exact copy of all faxes received.
- **Fax Machines II.** Receiving an after hours fax transmission is similar to receiving mail without an envelope. Sensitive messages are routinely read by bored guards and workers roaming around the building burning up their overtime. Use a fax vault.
- **Cordless Microphones.** Presenters at meetings love using them. Unfortunately, they transmit crystal clear audio about a quarter mile. Ban them from any meeting to which the general public would not be invited.
- **Dictation Machines.** You may shred the rough drafts, lock up the file copies, and send the originals in security sealed envelopes... but the dictation tape sits on the secretary's desk waiting to be swapped.

#7 – Meeting Chameleons

Off-site meetings, conventions, trade shows, seminars, etc. present the snoop with excellent opportunities for infiltration and information collection. Alert your people to the problems. Mention your protective actions...

- Off-site meetings... prime targets for snoops.
- Spy methods used may be unethical or illegal.
- Security will control meeting room access (24 hours).
- Electronic eavesdropping detection will be employed.
- Attendees must wear ID badges at all times.
- Never leave your laptop or briefcase unattended.
- Leave proprietary information with security.
- Proprietary data remains in the secured area.
- Do not discuss business in public areas.
- Be suspicious of strangers who befriend you.
- Report suspicious activity to security immediately.
- Define Proprietary Information.

It is information which is not general knowledge and is related to the company's products, methods, customers, plans, etc.

It is any information which would cause the loss of profit, or a competitive advantage, if it fell into the wrong hands.

#8 – The Silver Platter

Sometimes we just give information away. How many of the following items apply to someone you know?

- Unlocked offices, desks and file cabinets.
- Confidential paperwork left out overnight.
- Posted, shared or simpleton passwords.
- Phone directories which list everything but salary.
- Credit card, Social Security, and unlisted phone numbers posted in Rolodex® files left on desktops.
- Answering probing questions over the phone from people they don't really know.
- Sensitive topics discussed with known gossips.
- etc., etc., etc.

The list gets longer the more you think about it.

Solution: Think about it, the list will shorten.

#9 – Business Phone Attacks

Feature-rich business phones provide snoopers with a variety of powerful eavesdropping options. The phones themselves provide: electrical power; built-in microphones and speakers which can serve dual purposes; and ample hiding space for bugs and taps.

TELEPHONE SECURITY CHECKLIST...

- Provide high-level security for telephone rooms.
- Restrict direct dialing into the main telephone switch.
Some dangers of unauthorized phone system access include:
 - Complete deprogramming of the switch.
 - Secret reprogramming to allow access to...
free calls, voice mail, executive override features (which allow forced access busy extensions), bridge tap creation (allows silent monitoring from other extensions), hands-free intercom (allows room monitoring from other phones), and monitoring of the station message detail recording which maintains a record of all phone calls.
Recommendation: Replace the regular dial-up modem – which connects the switch to the outside line – with a call back type modem. With this configuration, PBX connections are limited to authorized phone numbers.
- Secure the on-site programming terminals.
- Be sure the System Administrator is trustworthy.
- Conduct periodic inspections for wiretaps.
- Conduct surprise audits of the software settings.
- Remove all unused wiring from sensitive areas.
- Make sure that voice mail and switch access passwords are high quality.
- Ask phone system users to report all suspicious calls and voice mail aberrations to the security department immediately.
In addition to snooping, these may also be indications of hackers trying to enter to steal services.



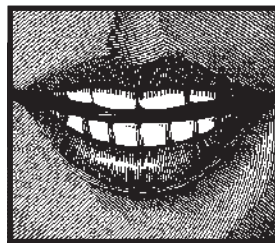
#10 – Treason

Another type of spy - the trusted employee - is one of the most dangerous and hardest to spot. The most likely candidates are employees who may...

- Be disgruntled, possibly related to insufficient raises, promotions, etc.
- Have incurred large debts due to gambling habits, unavoidable personal circumstances, or drug use.
- Be involved with labor / management issues.
- Have entrepreneurial personalities.

PROTECTION TIPS...

- Inspect for eavesdropping devices. These people have the time and opportunity to place and monitor.
- Selectively drop false bits of information and watch to see where they surface.
- Conduct background checks on all new employees and periodic checks on anyone with access to sensitive information.
 - Check previous employment carefully.
 - Uncover periods of employment not mentioned.
 - Verify periods of unemployment.
 - Living beyond their means may indicate extra income paid by the recipient of your business secrets.



THE GOOD NEWS...

Espionage is preventable, and knowing a snoop's tactics is the first step toward obtaining protection. You now have enough knowledge to begin that process confidently.

Spy Profile



What does a spy look like?

There is no exact answer.

However, a composite picture was developed by the Business Espionage Controls and Countermeasures Association...

- 21-35 years old. Female as often as male.
- College graduate with a low-value degree.
- Broad, short-term employment background.
- Money problems - low pay, poor self management.
- Military intelligence experience.
- Acquaintances with law enforcement backgrounds.
- Considered an outsider or loner.
- Disability precluding a law enforcement career.
- No police record prohibiting sensitive employment.
- Has driver's license, possibly a poor driving record.
- Romantic hobby or interests.
(Writer, photographer, sky diver, scuba, skiing, etc.)
- Collects underground & paramilitary literature.
- An active interest in firearms, often with training.
- Recruited from a want ad for Investigative Trainee.
- Often just a drone of a professional handler.
- Abilities in music, chess, math, etc. — skills associated with code breaking and espionage.

Keep this list in mind, but remember...

Your snoop could be anybody.

ABOUT THE AUTHOR...

Kevin D. Murray - CPP, CFE, BCFE has been solving electronic eavesdropping, security and counterespionage matters for business and government since 1973.

His many written works include: the Electronic Eavesdropping Detection chapter of The Protection of Assets Manual; articles for Security Management magazine; and Electronic Eavesdropping Detection and Industrial Espionage – The Missing Business School Courses.

His course - Electronic Eavesdropping Detection & Industrial Espionage was created for the John Jay College of Criminal Justice in New York.

Mr. Murray is a board member of the International Association of Professional Security Consultants, and is a Board Certified Forensic Examiner.

Although he complains about being too busy, there always seems to be time for his call-here-first-when-ever-you-have-a-technical question policy.

He may be reached at 908-832-7900, at P.O. Box 668, Oldwick, NJ 08858 (USA), or via murray@spybusters.com

Murray Associates services are available throughout North America and selected foreign countries.



MANAGEMENT CONSULTANTS TO
BUSINESS & GOVERNMENT ON
ELECTRONIC EAVESDROPPING DETECTION
& BUSINESS ESPIONAGE PREVENTION

P.O. BOX 668, OLDWICK, NJ 08858 (USA)
908 • 832 • 7900 • 800 • 635 • 0811

Capabilities information — www.spybusters.com
(Services available throughout the U.S. and selected foreign countries.)